Digitalisierung, Internet of Things, WEB 4.0 versus Sicherheitsmanagement, Datenschutz und rechtliche Anforderungen

Inhalt

Digitale Herausforderung

Bedrohungslage

Anforderungen

Umsetzungen in der Praxis

Inhalt

Die digitale Herausforderung

Die Bedrohungslage

Die Anforderungen

Die Umsetzungen in der Praxis

Internet der Dinge

Die Marktforscher von IDC schätzen, dass 2020 weltweit rund 30 Milliarden „Dinge“ – wie etwa Maschinen, Autos, Waschmaschinen und Kühlschränke – über das Internet vernetzt sein werden.

Digitalisierung

IT Mega Trends

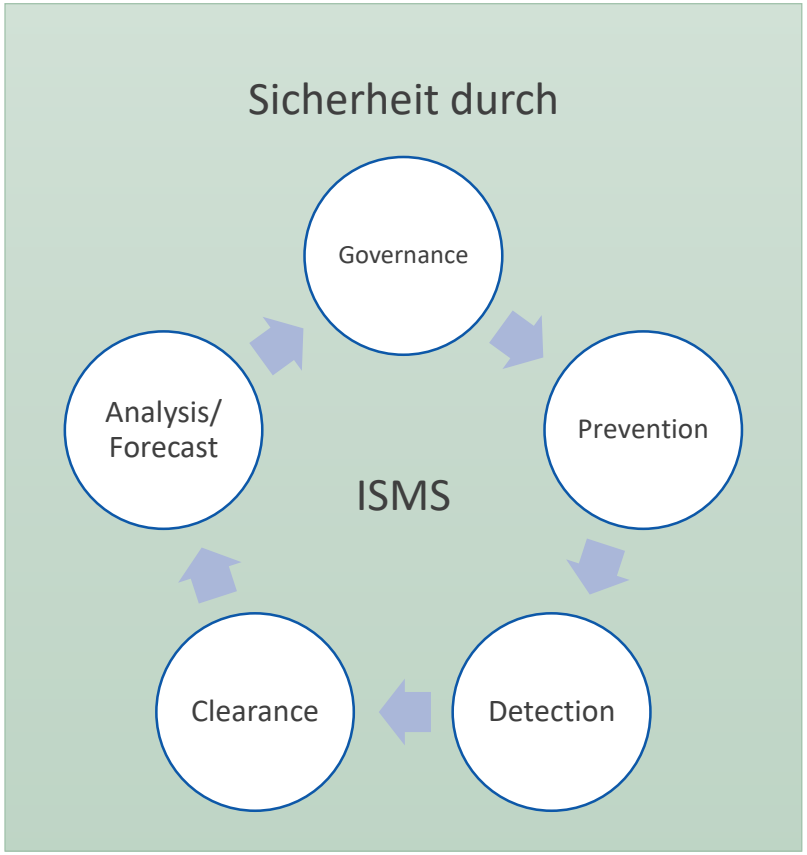
Wirtschaft 4.0
- Digitalisierung des Business
- Internet der Dinge (IoT)
- Maschine zu Maschine Kommunikation

Cloud
- Public / privat
- Provider & Datenhaltung
- Zusatznutzen

Social Media
- Kontextbasierte Multimedia-Konnektivität
- Arbeitslebensintegration und -verhalten
- Neue Wege der elektronischen Kommunikation

Big Data
- „Moores Law“ gilt ungebrochen (storage, memory)
- Ultraschnelle semantische Information Analysen
- Technische & Organisatorische Aspekte

Cyber Crime
- Fokussiert auf Gesellschafts- und Wirtschaftskriminalität
- Angriffe auf Service & Support Strukturen
- Angriffe aus Smart Building Konzept



Inhalt

Die digitale Herausforderung

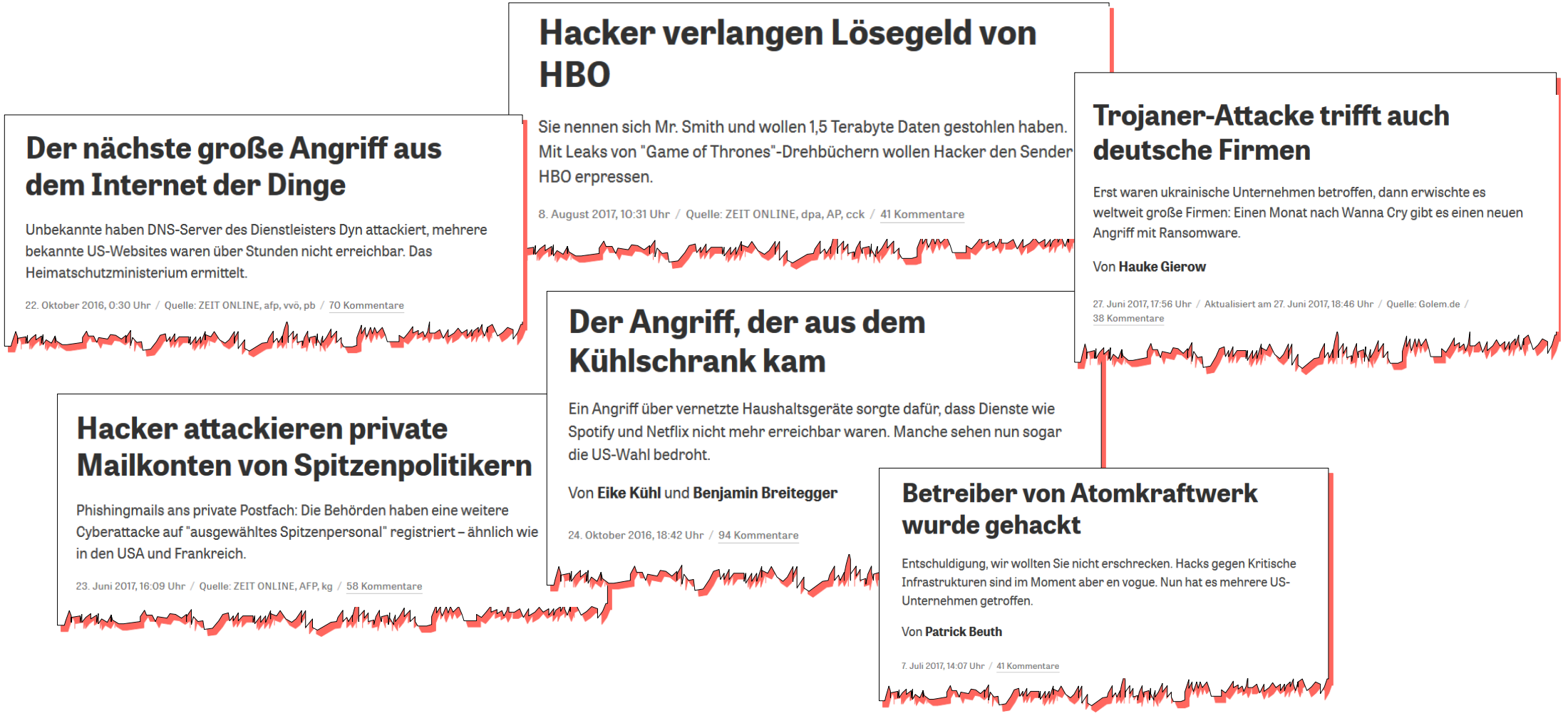
Die Bedrohungslage

Die Anforderungen

Die Umsetzungen in der Praxis

Wo viel Licht ist, ist starker Schatten

Jüngste IT-Sicherheit-Vorfälle



Der nächste große Angriff aus dem Internet der Dinge

Unbekannte haben DNS-Server des Dienstleisters Dyn attackiert, mehrere bekannte US-Websites waren über Stunden nicht erreichbar. Das Heimatschutzministerium ermittelt.

22. Oktober 2016, 0:30 Uhr / Quelle: ZEIT ONLINE, afp, vvö, pb / 70 Kommentare

Hacker verlangen Lösegeld von HBO

Sie nennen sich Mr. Smith und wollen 1,5 Terabyte Daten gestohlen haben. Mit Leaks von "Game of Thrones"-Drehbüchern wollen Hacker den Sender HBO erpressen.

8. August 2017, 10:31 Uhr / Quelle: ZEIT ONLINE, dpa, AP, cck / 41 Kommentare

Trojaner-Attacke trifft auch deutsche Firmen

Erst waren ukrainische Unternehmen betroffen, dann erwischte es weltweit große Firmen: Einen Monat nach Wanna Cry gibt es einen neuen Angriff mit Ransomware.

Von **Hauke Gierow**

27. Juni 2017, 17:56 Uhr / Aktualisiert am 27. Juni 2017, 18:46 Uhr / Quelle: Golem.de / 38 Kommentare

Hacker attackieren private Mailkonten von Spitzenpolitikern

Phishingmails ans private Postfach: Die Behörden haben eine weitere Cyberattacke auf "ausgewähltes Spitzenpersonal" registriert – ähnlich wie in den USA und Frankreich.

23. Juni 2017, 16:09 Uhr / Quelle: ZEIT ONLINE, AFP, kg / 58 Kommentare

Der Angriff, der aus dem Kühlschrank kam

Ein Angriff über vernetzte Haushaltsgeräte sorgte dafür, dass Dienste wie Spotify und Netflix nicht mehr erreichbar waren. Manche sehen nun sogar die US-Wahl bedroht.

Von **Eike Kühl** und **Benjamin Breitegger**

24. Oktober 2016, 18:42 Uhr / 94 Kommentare

Betreiber von Atomkraftwerk wurde gehackt

Entschuldigung, wir wollten Sie nicht erschrecken. Hacks gegen Kritische Infrastrukturen sind im Moment aber en vogue. Nun hat es mehrere US-Unternehmen getroffen.

Von **Patrick Beuth**

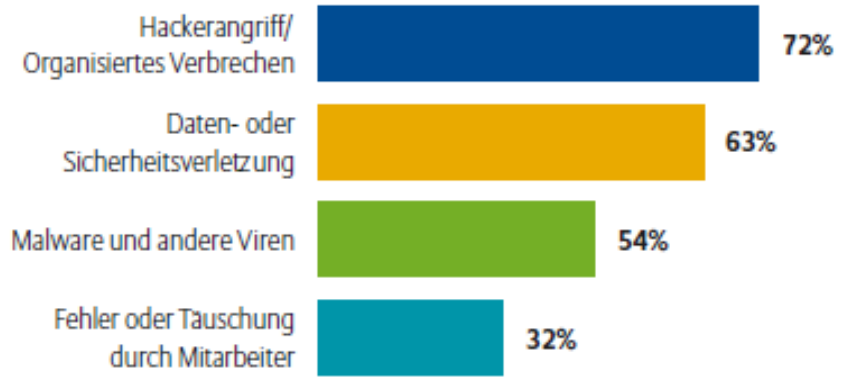
7. Juli 2017, 14:07 Uhr / 41 Kommentare

Quelle: Zeit Online

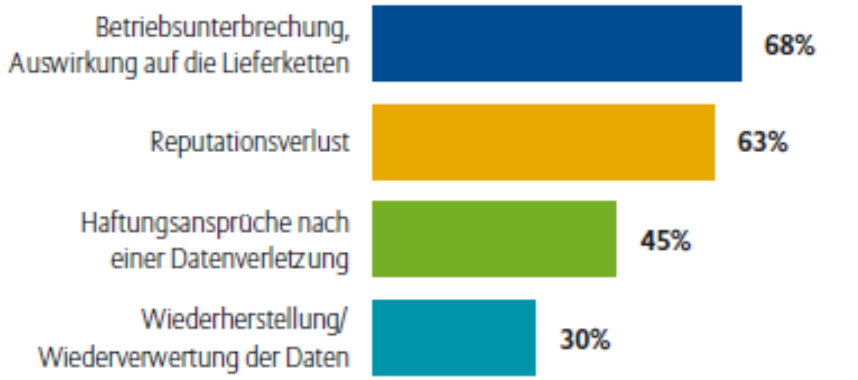
Top Risiko im Fokus - Cybervorfälle

Warum Cybervorfälle ein immer größeres Risiko werden

Was sind die Hauptursachen für Cybervorfälle?

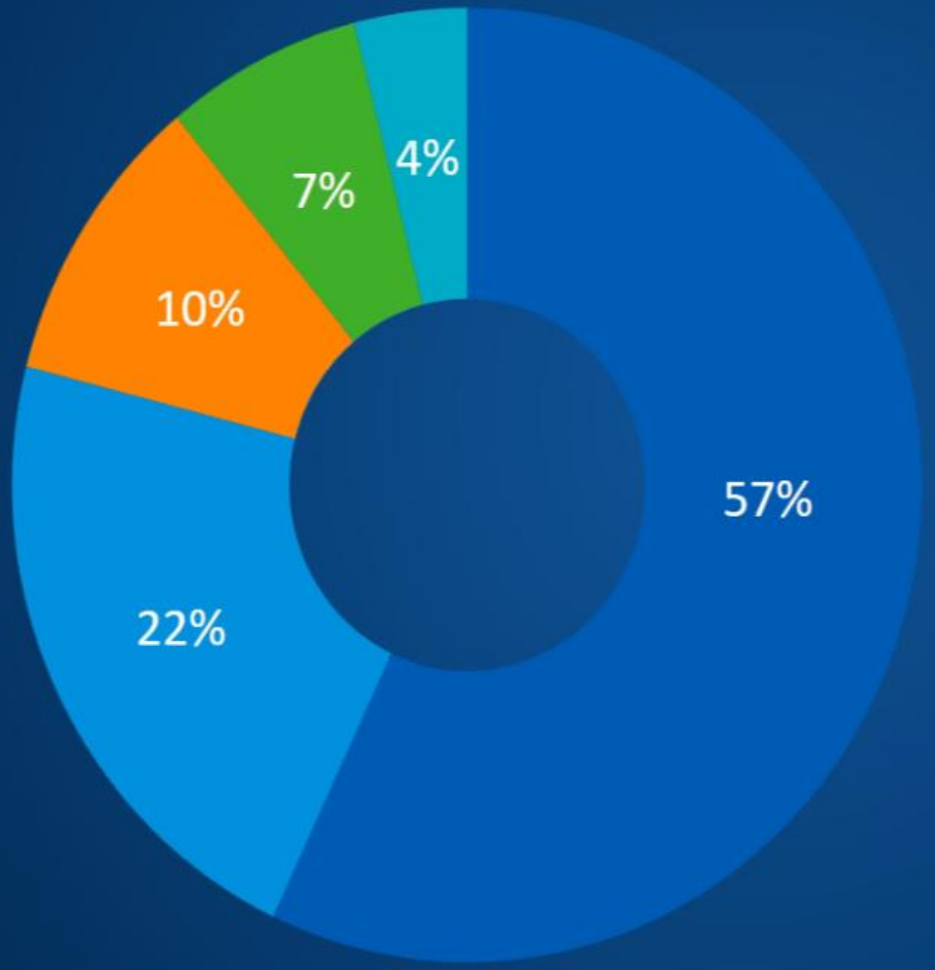


Was sind die Hauptursachen für den wirtschaftlichen Verlust nach einem Cybervorfall?



Quelle: Allianz Global Corporate & Specialty

Hauptursachen für Datenabfluss



- Hacking und Malware
- Unbeabsichtigtes Teilen
- Portable Geräte
- Physischer Verlust
- Andere

SOPHOS

2016 Data Breaches – Privacy Rights Clearinghouse

Wichtigste Unternehmensrisiken 2017 in Deutschland

Deutschland

Top-Risiko Cybervorfälle

▲ Politische Risiken (Krieg, Terror)

▲ Neue Technologien

„Die zunehmende Vernetzung in einer Industrie 4.0-Umgebung sowie die Raffinesse von Cyberattacken stellen ein großes Risiko für deutsche Unternehmen dar. Wir sehen mehr Regulierung durch Gesetzgeber und ein wachsendes Risikobewusstsein im Top-Management. Immer mehr Unternehmen entwickeln gezielte Cyber-Abwehrstrategien."

Andreas Berger, CEO, AGCS Zentral- und Osteuropa

Quelle: Allianz Global Corporate & Specialty

Risiken der Digitalisierung

Steigende Anforderung an die Datensicherheit

Sabotage, Datenklau, Hackerangriffe

Veränderung der Geschäftsmodelle

Verlust der Privatsphäre

Wachsender Investitionsdruck

Kontrollverlust

Steigender Wettbewerb

Arbeitslosigkeit

Omnimetrie
"Die Sucht oder die Notwendigkeit, alles zu messen."

Inhalt

Die digitale Herausforderung

Die Bedrohungslage

Die Anforderungen

Die Umsetzungen in der Praxis

IT-Sicherheitsgesetz

- Am 25.07.2015 in Kraft getreten
- Am 03.05.2016 erste BSI-KRITIS-Verordnung oder Rechtsverordnung (RVO) bekannt als
- 1. RVO-Korb für
  - Energie: Elektrizität, Gas, Mineralöl
  - Wasser: Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung
  - Ernährung: Ernährungswirtschaft, Lebensmittelhandel
  - Informationstechnik und Telekommunikation
- 2. RVO-Korb wird 2017 erwarten für
  - Transport und Verkehr
  - Gesundheit
  - Finanz- und Versicherungswesen

Was muss ich als KRITIS-Betreiber tun?

Bundesamt
für Sicherheit in der
Informationstechnik

LEICHTE SPRACHE

Themen | Das BSI

Industrie und Kritische Infrastrukturen

Was muss ich als KRITIS-Betreiber tun?

Betreiber Kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes sind nach Verabschiedung der BSI-Kritisverordnung verpflichtet,

- eine Kontaktstelle zu benennen,
- IT-Störungen zu melden,
- den „Stand der Technik“ umzusetzen.

Um KRITIS-Betreibern die Erfüllung dieser Pflichten möglichst einfach zu machen, erhalten sie auf den folgenden Seiten konkrete Informationen zur Umsetzung der genannten Punkte.

nützliche Erklärung

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

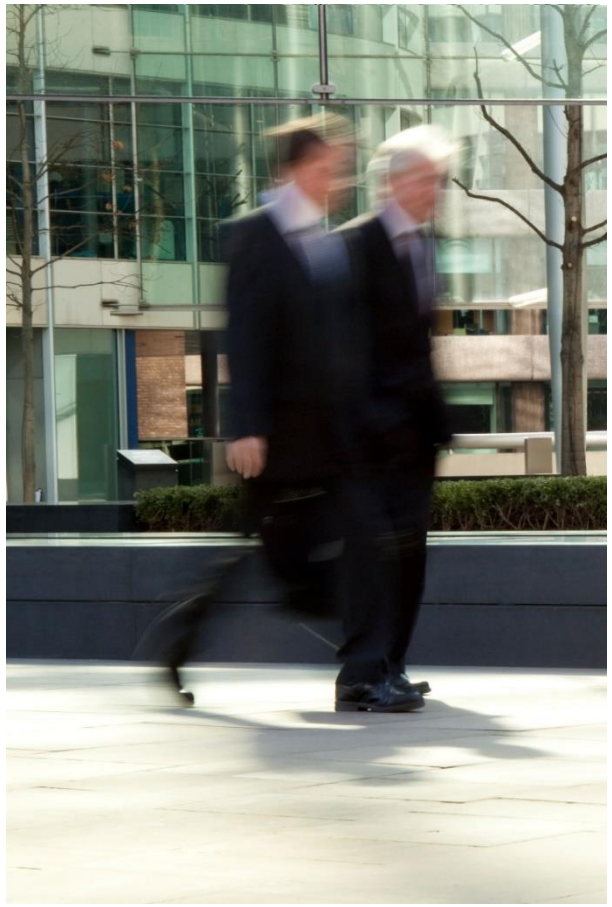
TeleTrusT
Pioneers in IT security.

Handreichung
zum "Stand der Technik"
im Sinne des
IT-Sicherheitsgesetzes (ITSiG)

WMC
Wüpper Management Consulting

IT-Sicherheit bei KRITIS-Unternehmen - eine unmittelbare Geschäftsführungsaufgabe

Anforderungen des IT-Sicherheitsgesetztes an Vorstände und Geschäftsführer – was ist neu?



- **Worauf zielen die neuen Gesetze und Regelungen ab?**
  Die neuen Gesetze und Regelungen gelten für den Schutz Kritischer Infrastrukturen (KRITIS) – d.h. Organisationen mit wichtiger Bedeutung für staatliche Gemeinwesen, deren Ausfall oder Manipulation massive Auswirkungen auf die Versorgung der Bevölkerung und die Sicherheit haben könnten.

- **Was ist zu tun?**

  – Meldepflicht: sämtliche IT-Sicherheitsvorfälle müssen an das BSI gemeldet werden.

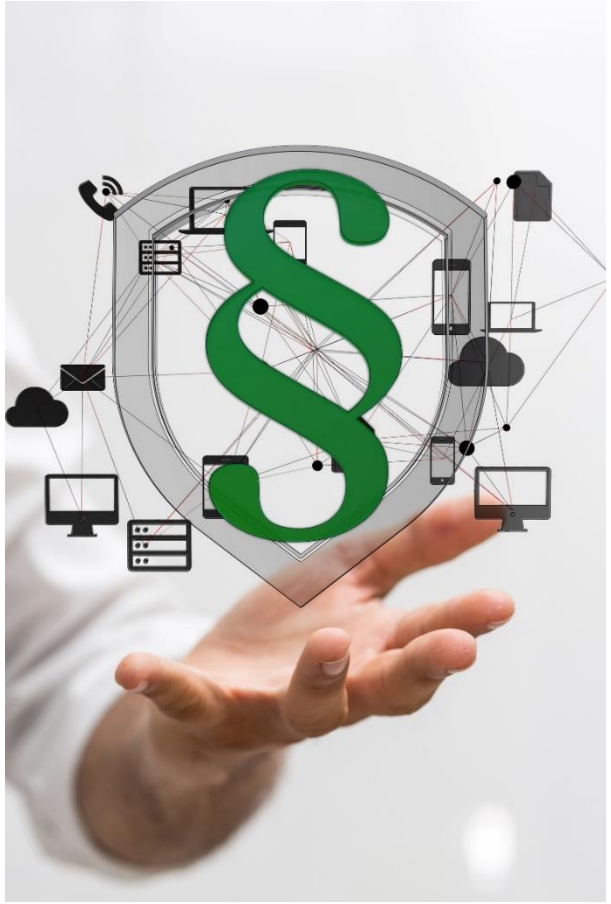
  – Mindeststandards der Informationssicherheit auf Basis des BSI IT-Grundschutzes oder der ISO 27001 einhalten.

  – Regelmäßige Nachweise: Prüfungen sowie Zertifizierungen werden von nachweislich qualifizierten Zertifizierungsstellen und Prüfern durchgeführt.

  – Ab Veröffentlichung der Rechtsverordnung für die jeweilige Branche (siehe nächste Seiten) haben Sie zwei Jahre Zeit, Ihre IT nach dem Stand der Technik abzusichern d.h. ein Information Security Management System (ISMS) einzuführen, zu betreiben und regelmäßig testieren zu lassen.

IT-Sicherheit bei KRITIS-Unternehmen - eine unmittelbare Geschäftsführungsaufgabe

Die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) – welche Sektoren zählen zu KRITIS?



- **Welche Unternehmen fallen unter das IT-Sicherheitsgesetz?**
  - **3. Mail 2016** - der erste Teil der Verordnung wurde veröffentlicht. Hier wurde im ersten Schritt für die Sektoren Energie, Wasser, Informationstechnik und Telekommunikation sowie Ernährung bestimmt, welche Dienstleistungen und deren Anlagen wegen ihrer Bedeutung als kritisch anzusehen sind.
  - **Ende 2017** - der zweite Teil der KRITIS-Verordnung mit den Sektoren Finanzen, Transport und Verkehr sowie Gesundheit wird erwartet.
  - **Mehr Details finden Sie hier:** https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/kritis-vo-kabinett.pdf?__blob=publicationFile

IT-Sicherheit bei KRITIS-Unternehmen - eine unmittelbare Geschäftsführungsaufgabe

Anforderungen des IT-Sicherheitsgesetztes an Vorstände und Geschäftsführer – worauf müssen Sie achten?

- **Welche Standards sind für das ISMS gültig?**
  - **DIN ISO/IEC 27001:** Das Information Security Management System (ISMS) eines KRITIS-Unternehmens muss an der ISO 27001 ausgerichtet sein. Die ISO 27001 umfasst die allgemeinen Inhalte und Anforderungen an ein ISMS bezüglich der Verfügbarkeit, Vertraulichkeit und Integrität kritischer Daten. Ferner verpflichtet ein ISMS nach ISO 27001 das Management eines Unternehmens, Sicherheitsrichtlinien und Regelungen zu erlassen und die erforderlichen Ressourcen bereit zu stellen.
  - **BSI IT -Grundschutz:** Als nationaler Standard für IT-Sicherheit spricht der IT-Grundschutz Handlungsvorgaben für die Umsetzung der Anforderungen an die Informationstechnologie aus.
  - **DIN ISO/IEC 27005:** Dieser internationale Standard ist eine Umsetzungsempfehlung zur Durchführung des Risikomanagements und erfüllt die Forderungen der ISO 27001. **Analog der BSI IT-Grundschutz 100-3**

IT-Sicherheit bei KRITIS-Unternehmen - eine unmittelbare Geschäftsführungsaufgabe

Anforderungen des IT-Sicherheitsgesetztes an Vorstände und Geschäftsführer – worauf müssen Sie achten?

- **Welche Standards sind für das ISMS gültig?**

Branchenspezifische Anforderungen an die Informationssicherheit. Diese Standards setzen auf die ISO/IEC 2700x oder BSI IT-Grundschutz auf und erweitern die Vorgaben an ein ISMS um die typischen Aspekte jeweiliger Branche.

- **ISO/IEC 27011**: ISMS für Telekommunikationsunternehmen
- **ISO/IEC TR 27015**: ISMS für den Finanzsektor (Banken etc.)
- **ISO/IEC 27017** und **ISO/IEC 27018:** Leitfaden für Cloud-Dienste
- **ISO/IEC TR 27019:** ISMS für Energieunternehmen
- **EN ISO/IEC 27799**: ISMS für das Gesundheitswesen
- **BSI IT-Grundschutz / Leitfaden Wasserwirtschaft**: ISMS für die Wasserwirtschaft

Energieversorger / Wasserwirtschaft

Kritische Infrastrukturen

Energieversorger

- ISO/IEC 27001 - ISMS
- ISO/IEC 27019 - erweiterte Anforderungen
- ISO/IEC 27005 - Risikomanagement

- Bewertung der Anforderungen (Controls)
- Risikomanagement nach Bedrohungen und Schwachstellen

Wasserwirtschaft

- BSI IT-Grundschutz - ISMS
- Leitfaden - erweiterte Anforderungen
- Leitfaden - Risikomanagement (Basis BSI 100-3)

- Bewertung von Anwendungsfällen und Maßnahmenvorgaben
- Risikomanagement nach Gefährdungen und nicht umgesetzten Maßnahmen

IT-Sicherheitsgesetz

Anwendungsbereich im Finanzsektor

§ 2 Begriffsbestimmungen

(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

§ 8c Anwendungsbereich

(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EC der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden.

Betroffene Betreiber / Relevante Dienstleistungen

Was könnte im Finanzsektor „kritisch“ sein?

Ressorts	BaFin	BSI-Sektorstudie*
Zahlungsverkehr • Kartenzahlung • Überweisung • E-Geld	Zahlungsverkehr • Kartenzahlung • Online-Banking (einschl. Mobile-Banking)	Zahlungsverkehr • Kartenzahlungen • Abwicklung bargeldlosen Zahlungsverkehrs
Bargeldversorgung	Bargeldversorgung	Bargeldversorgung
Wertpapier- und Derivatehandel		Wertpapier- und Derivatehandel
Kreditvergabe		
Geld- und Devisenhandel		
Versicherungsleistungen		
	Dienstleistungen, bei denen Vorfälle zu einer Verletzung der Vertraulichkeit analog § 42a BDSG oder zu signifikanten Reputationsschäden führen können oder die vom Institut als Notfall gewertet werden	

Branchenstandard

Abgleich Anforderungen Standards

Branchenstandard-anforderung / ISO-Standard	27001	27002	27015
Anforderungen aus dem Gesetzestext			
• Festlegung von Schutzzielen	✓✓	✓✓	✗
• Ableitung der Schutzziele aus KRITIS-Forderungen	✗	✗	✗
• Prüfschema	✓	✗	✗
Anforderungen an inhaltliche Ausrichtung			
Abstraktionsgrad			
• Abzudeckende Themen und Detailtiefe	✗	✓	✓✓
Anforderungen an das Risikomanagement			
Anforderungen an im Standard abzudeckende Themen			
• ISMS	✓✓	✓✓	✓✓
• Branchenspezifische Technik	✗	✗	✓✓
Anforderungen an Maßnahmen, die folgenden Bedrohungen und Schwachstellen begegnen			
• Bedrohung: Unbefugter Zugriff	✗	✗	✓
• Schwachstelle: Menschliches Fehlverhalten	✗	✗	✗
Wirtschaftlichkeit und Skalierbarkeit			

EU-Datenschutzgrundverordnung (EU DS-GVO)

(1) Personenbezogene Daten müssen …
… („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)
… („Zweckbindung“)
… („Datenminimierung“)
… („Richtigkeit“)
… („Speicherbegrenzung“)
… **geeignete technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit“)

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen **Einhaltung nachweisen können** („**Rechenschaftspflicht**“).

EU-Datenschutzgrundverordnung (EU DS-GVO)

- Strukturierte Erfassung der datenschutzrelevanten Prozesse im Unternehmen
- Auf Basis dieser Prozesse ist eine Risikoanalyse sowie eine Datenschutz-Folgenabschätzung durchzuführen
- Entsprechend dem bestehenden Risiko sind Betriebe verpflichtet, "technische und organisatorische Maßnahmen" zu ergreifen
- Rechte der Betroffenen
- Anzeigepflicht

Wer die hier getroffenen Regeln verletzt, muss mit heftigen Sanktionen von bis zu 20 Mio. Euro beziehungsweise 4 Prozent des weltweiten Jahresumsatzes rechnen.

Alle Unternehmen, die bereits ein funktionierendes **Informationssicherheits-Managementsystem nach ISO 27001** eingeführt haben, sind hier im **Vorteil**.

Informationssicherheit & Datenschutz

Integrative Betrachtung

Informationssicherheit

Geschäftsprozesse

Informationen

Assets

Risikomanagement

Office Infrastruktur

Information Security Mgmt.
Keine gesetzlichen Vorgaben
Etablierte Vorgaben
- ISO/IEC 27001 & ff
- BSI
- …

?

Kritische Infrastruktur

IT-Sicherheitsgesetz 2015
Produktionsumgebungen
Erweiterte Vorgaben
- ISO/IEC 27019*
- BSI*

01/2018

Datenschutz 05/2018

Verfahren

Personenbezogene Daten

Assets

Risikomanagement

Die Datenschutz-Grundverordnung (DSGVO)

- Inkrafttreten am 25.05.2018, zwei Jahre nach Verkündung
- Keine (weitere) Übergangsfrist
- Wirkungen:
  - Europaweit einheitliches Datenschutzrecht
  - Vollharmonisierung, aber „Öffnungsklauseln“ für Konkretisierungen der Mitgliedstaaten
  - Unmittelbar
  - Löst nationales Datenschutzrecht (BDSG) ab
  - Verpflichtet Unternehmen und öffentliche Verwaltung

Vorgaben der Branchenverbände z. B. * Netzagentur ** Wasserverband

Inhalt

Die digitale Herausforderung

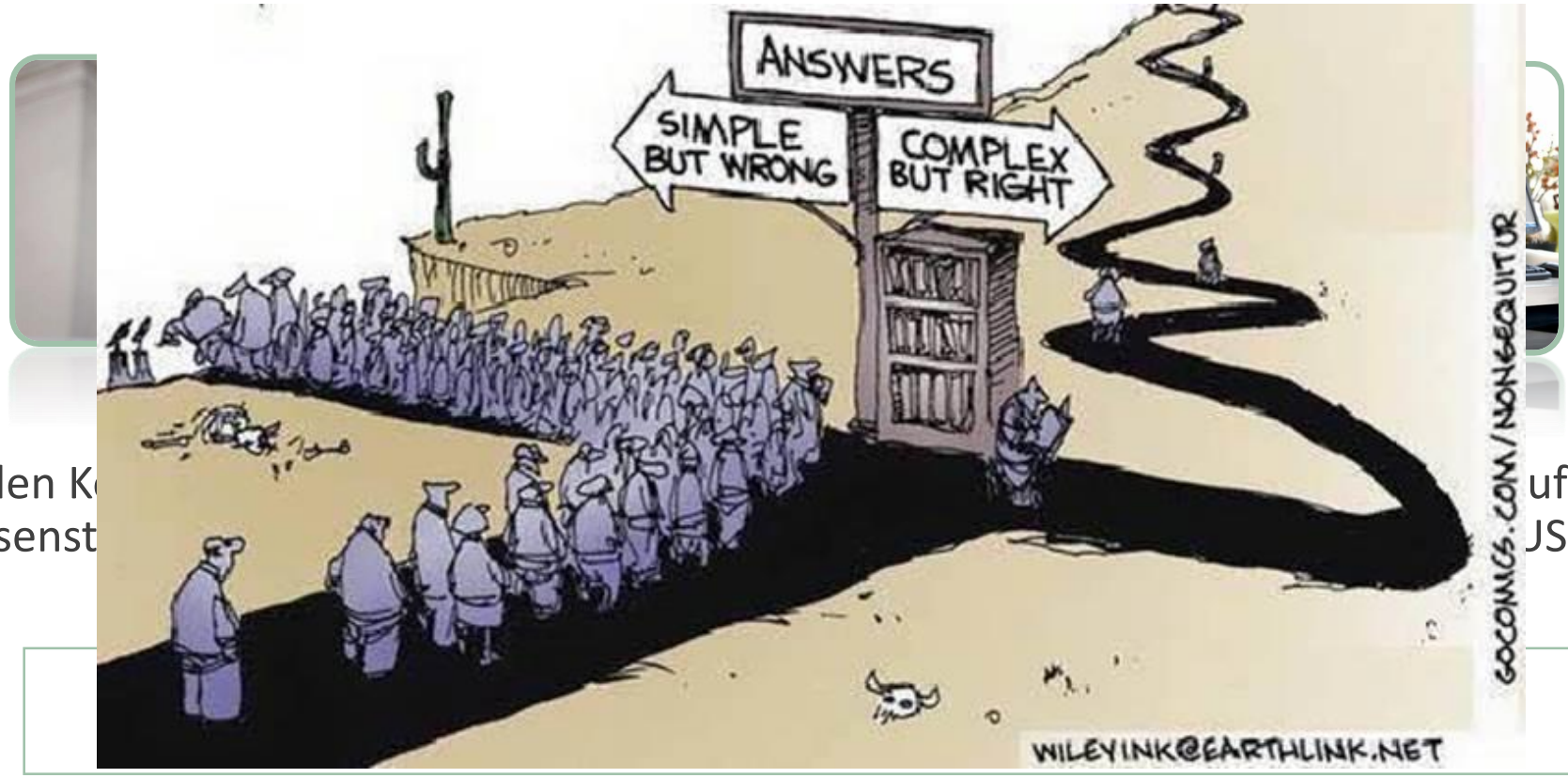
Die Bedrohungslage

Die Anforderungen

Die Umsetzungen in der Praxis

Einleitung: Informationssicherheitsmanagement

Informationen existieren in vielfältiger Art und Form ...

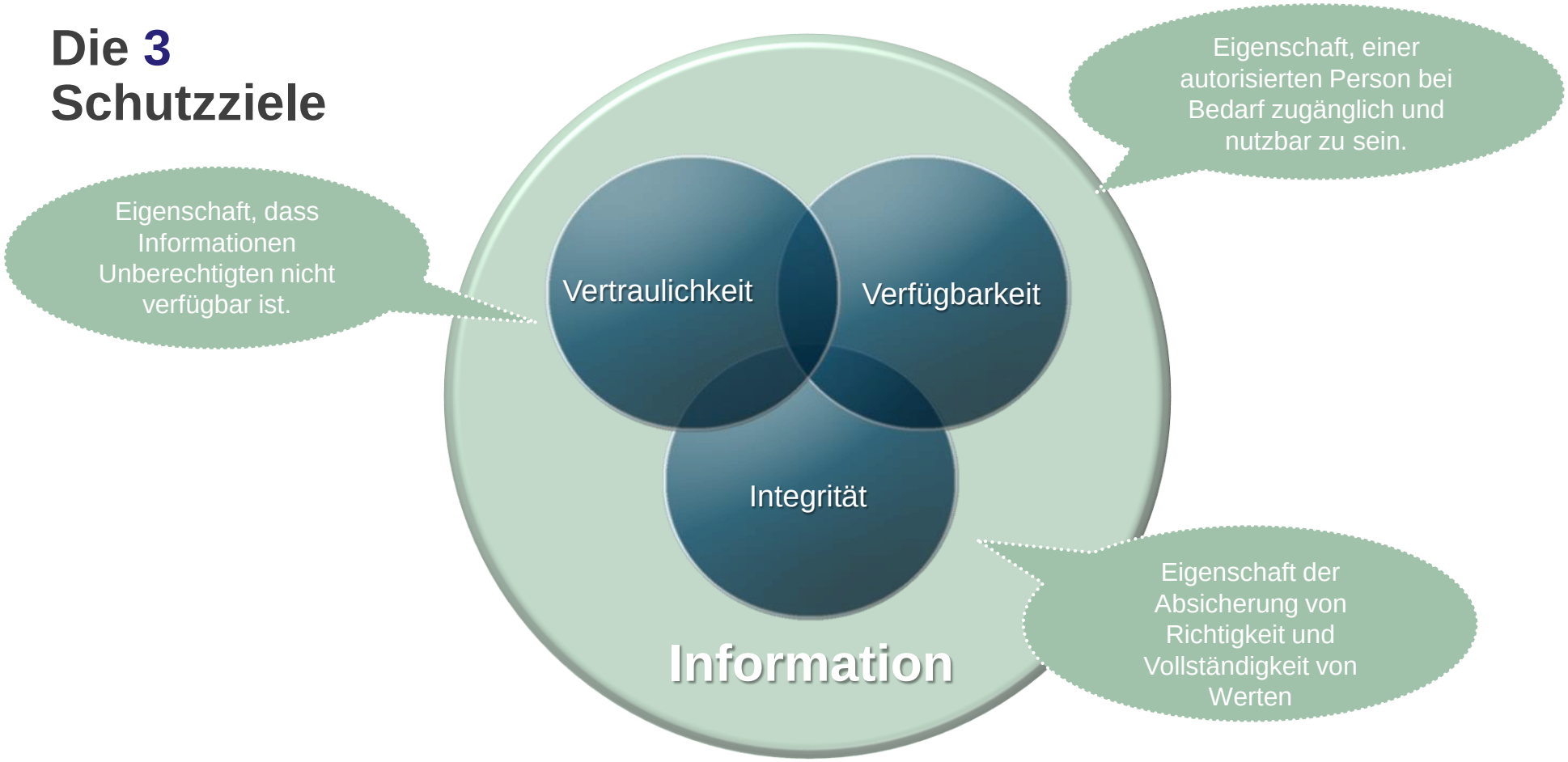


z.B. in den K uf Medien
„Wissenst JSB, DVD, ...)

Einleitung: Informationssicherheitsmanagement

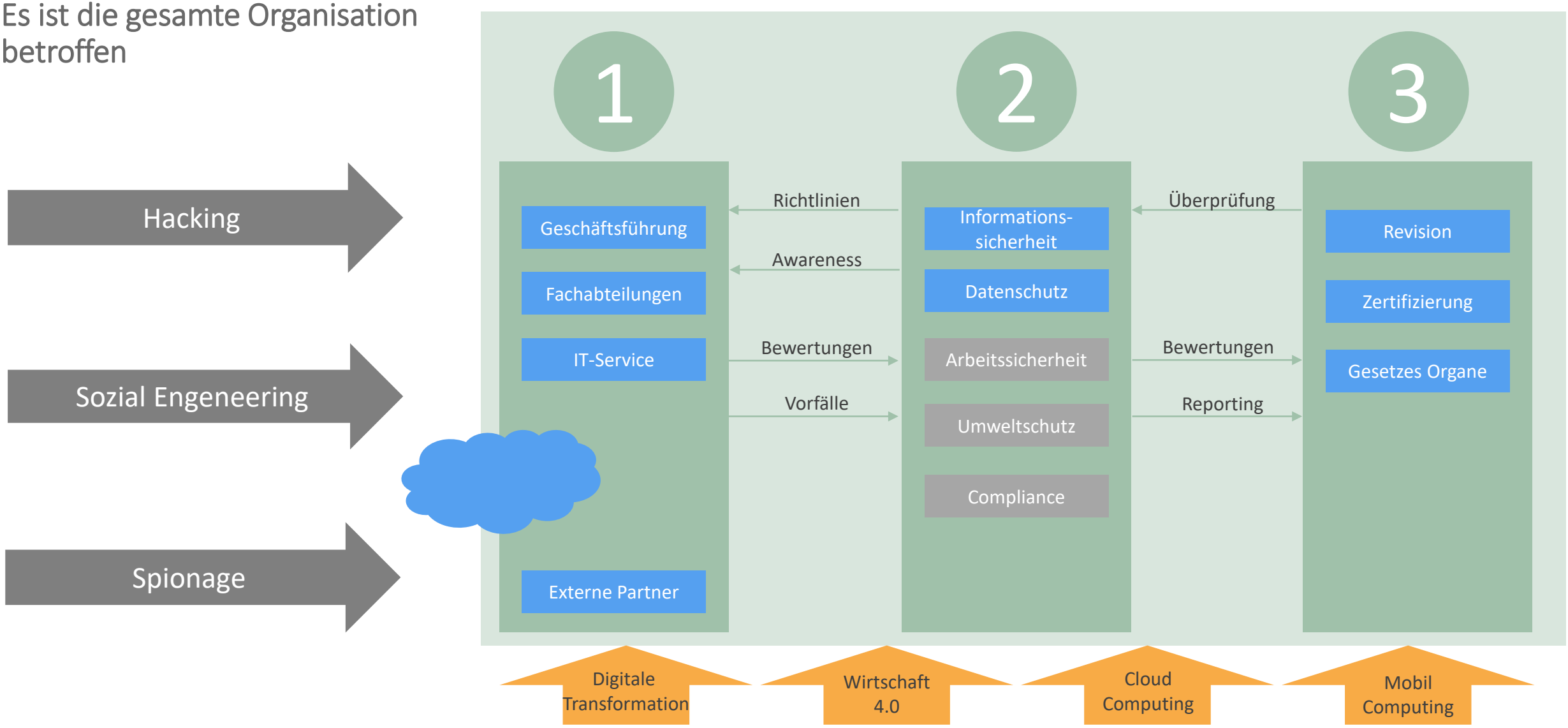
Die Schutzziele der Informationssicherheit

Die 3 Schutzziele



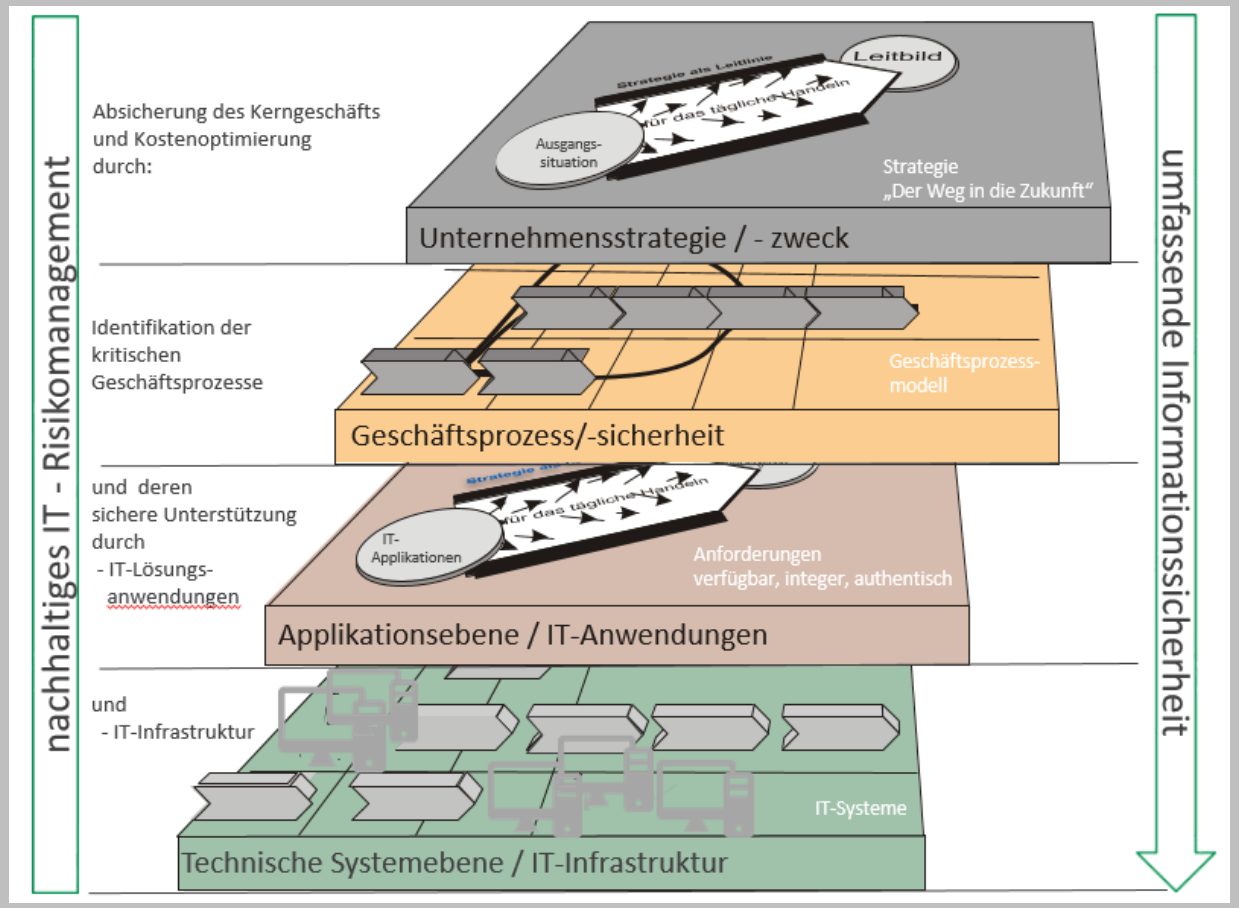
3 lines of defence

Es ist die gesamte Organisation betroffen



IT-GRC & ISMS!

ISMS - Einbindung auf allen Ebenen:



Unternehmensziele & IT-Ziele
Normen Controls & Fragekataloge
ISMS Scope & IS-Framework nach den Normen-Controls

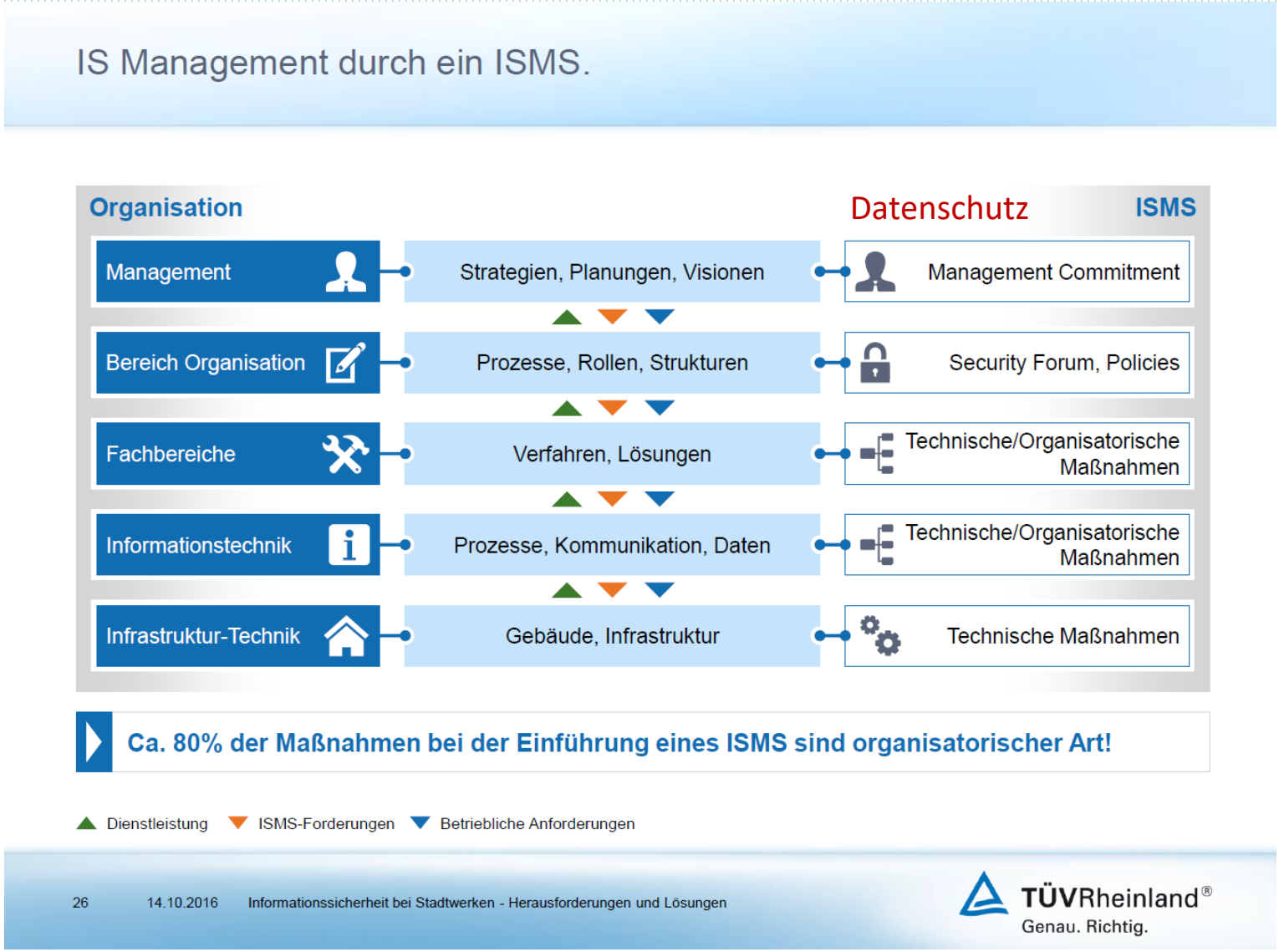
Geschäftsprozesse / IT-Serviceprozesse
Informationsbewertung nach V,I,V & Datenschutzrelevanz

Informationen & Assets bewerten
Risikobewertung der Assets nach Bedrohungs- und Schwachstellenkatalogen / Gefährdungen

Strukturanalyse der Assets
Bewertung der Assets nach vorgegebenen IS-Anforderungen
Risikobewertung der Assets nach Bedrohungs- und Schwachstellenkatalogen

Mitarbeiterdaten / Organisation

Sicherheitskonferenz Strahlsund 2016 / Auszug



Quelle: TÜV Rheinland

Untersuchungsbereiche mit dem Fokus auf Informationssicherheit - klassisch

Informationssicherheit (nach ISO/IEC 27001 = IT-/Cyber Security + physikalischer Schutz + Absicherung des Geschäftsbetriebes (+ Datensicherheit)

Untersuchungsbereich Office-Umgebung

Gemeinsamer Untersuchungsbereich Datacenter

Untersuchungsbereich Industrieumgebung

Scope:
- Unternehmensorganisation
- Hauptsächlich Aktivitäten während der Regel-Arbeitszeit
- Businessprozesse und personelle Ressourcen
- Ganzheitliches Risikomanagement
- zentrale Systeme wie ERP, Mail/Exchange, Fileserver
- oft: IT Service- und Supportstrukturen, kaskadierendes Know-How
- **Vertraulichkeit**, Verfügbarkeit u. Integrität von Informationen

Scope:
- Plant-Organisation
- oft 24x7x365 Betrieb
- Wertschöpfungskette und technischen Ressourcen
- Operatives Risikomanagement
- dezentrale Industrielle ICS Systeme wie SCADA, DCS, PLC
- Leitstand-Organisation: tiefes Spezialwissen im „1st-Level“
- **Echtzeitfähigkeit,** Verfügbarkeit und Integrität von DATEN

Untersuchungsbereiche mit dem Fokus auf Informationssicherheit – HEUTE!

Herausforderungen der Zukunft wie Digitalisierungsvorhaben im Rahmen der Industrie 4.0 sowie Internet of Things IoT):

- Stärkere Vernetzung von Prozessen und Ressourcen führt zu integrierte Analyse und Nutzung von Informationen/Daten,
- die Zahl der Sensoren und der Grad der Interoperabilität zwischen IT und OT (Operational Technology; Betriebstechnik) nimmt stark zu

Bedrohungen für ICS:

- Attacken auf die Office-Welt (Viren, Würmer, Trojaner) greifen durch bis auf die Plant-Umgebung
- direkter Angriff auf Industrieanlagen aus dem Internet
- Nutzung aller industriell- genutzten Ethernet-Protokolle für den Transport von Schadware (siehe Stuxnet)
- Beseitigung technischer Schwachstellen im industriellen Umfeld „aufwendig“

Notwendigkeit gemeinsamer Regelungen zur ORGANISATORISCHEN Absicherung

Ableitung der „Organisation der Sicherheit“ aus der Unternehmensorganisation

Folgende Rollen und VERANTWORTLICHKEITEN sollten festgelegt werden:

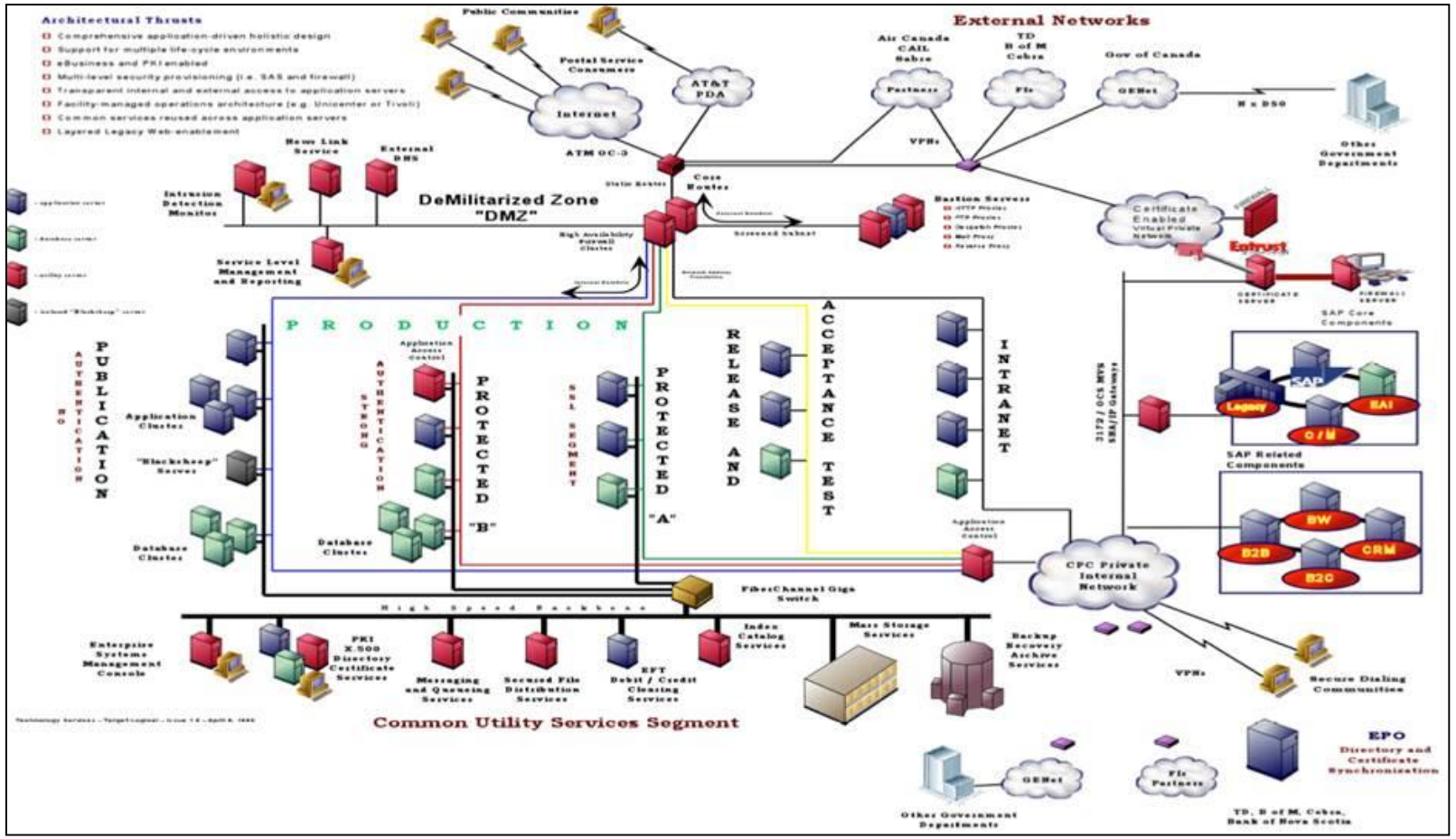
- Leiter der Informationssicherheit
- Risikomanager
- Compliance-Verantwortlicher
- Prozessverantwortliche in Office- und Industrieumgebung
- Systemverantwortliche im Datacenter-Umfeld
- Gemeinsame Krisenorganisation mit festgelegten Kompetenzen und Ressourcen

Folgende Prozesse und Methoden sollten festgelegt werden (Basics):

- Sensibilisierung und Schulung der Mitarbeiter
- Umgang mit Störungen (Incident-Management)
- Umgang mit technischen Veränderungen (Change-Management)

Blickwinkel ändern

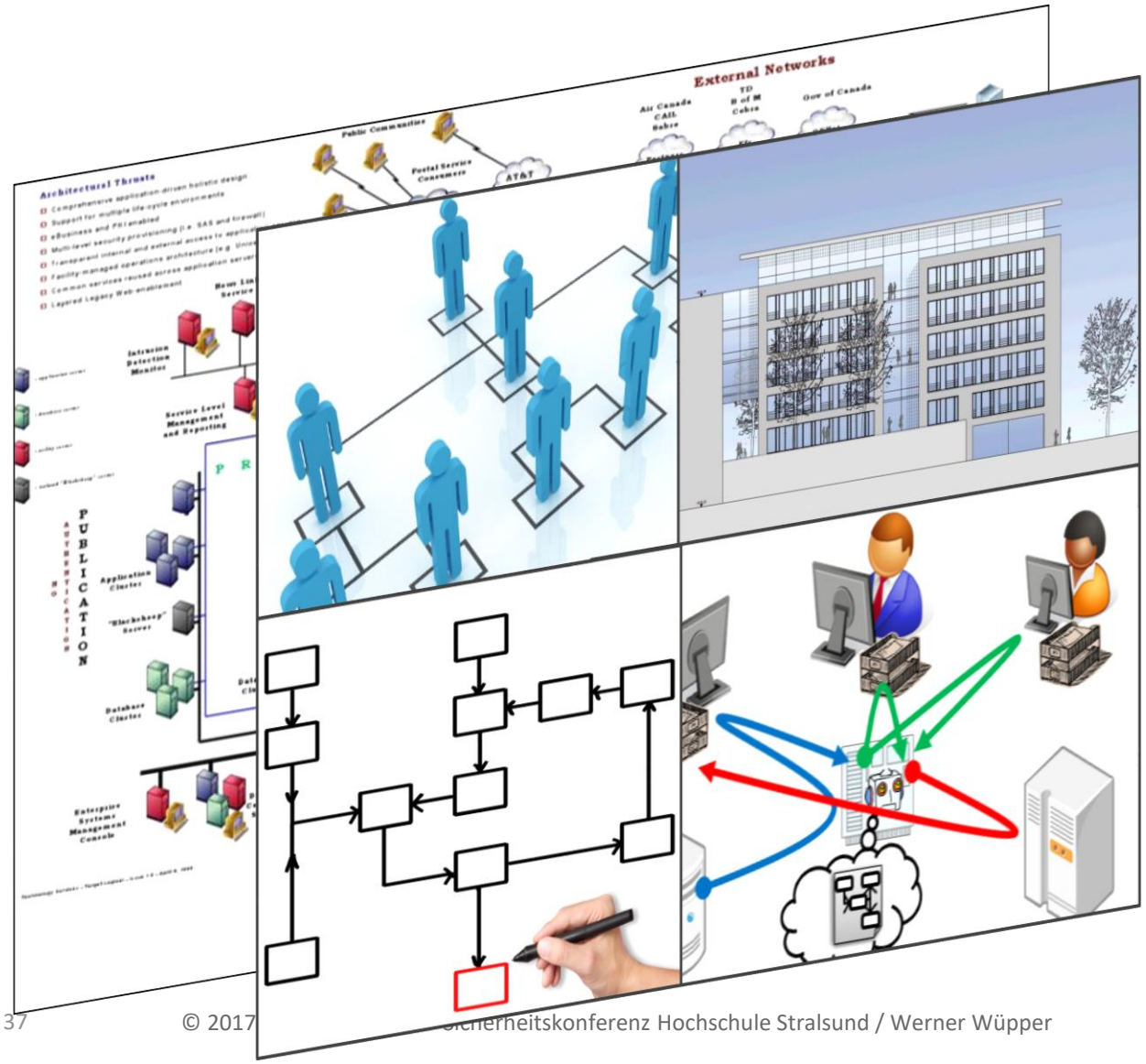
Die Betrachtung der Technik löst nicht die Aufgabenstellung



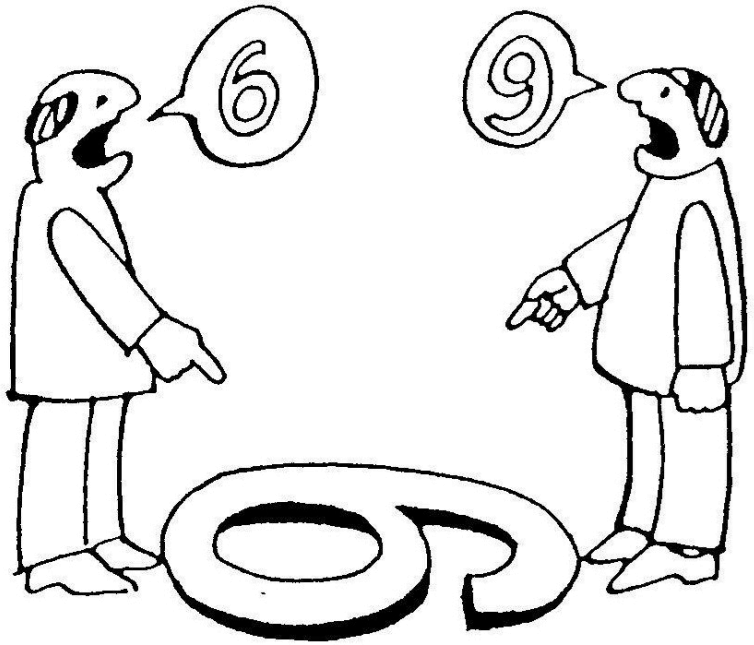
- Technische Absicherung der Informationstechnologie
  - Hard- und Software
  - IT-Sicherheit
  - IT-Administration
  - Cyber Security
  - Serviceprozesse

Blickwinkel ändern

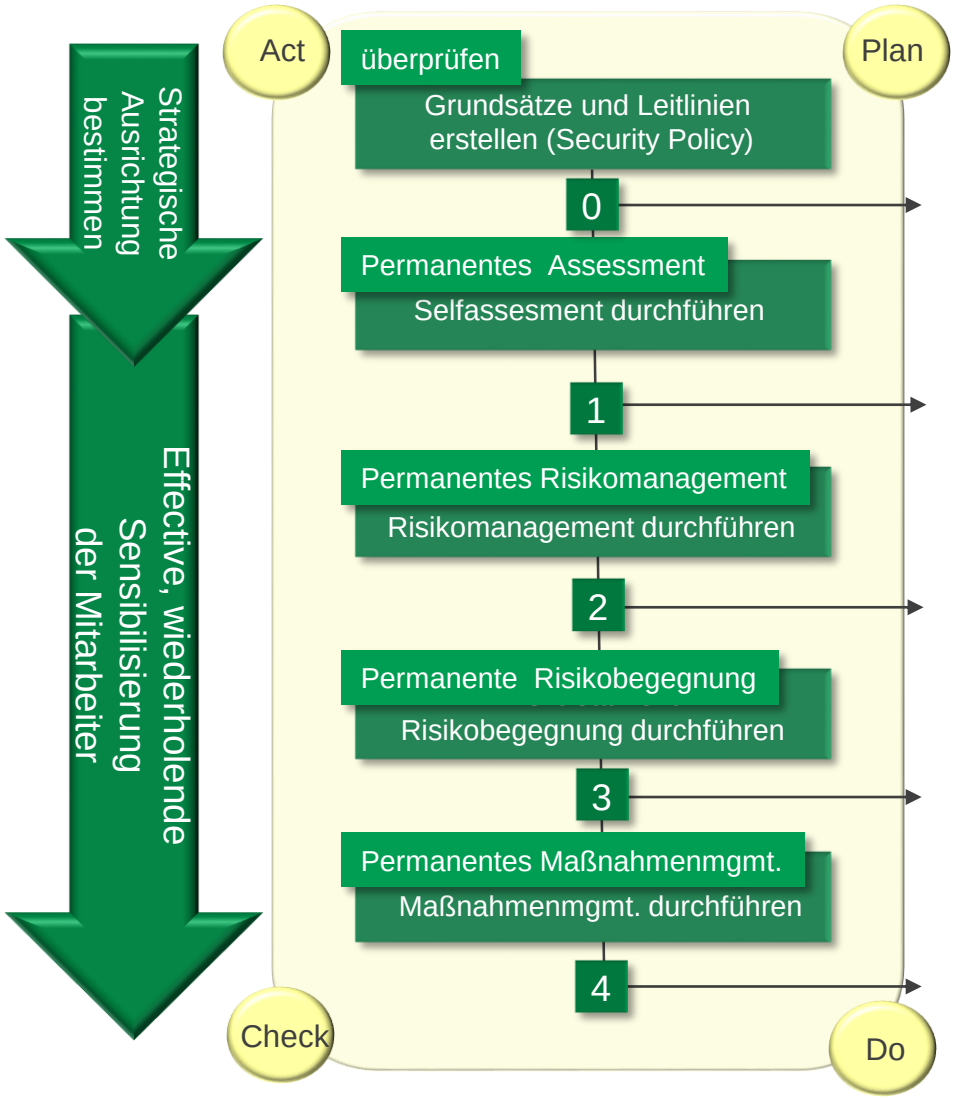
Die Betrachtung der Technik löst nicht die Aufgabenstellung



- Organisation
- Prozesse
- Menschen
  - Anwender
  - Administratoren
  - Externe Partner
- Infrastruktur



Vorgehen zur Regelung ORGANISATORISCHER Absicherung



Methode zum Betrieb eines ISMS

- **Geschäftsführungsentscheidung zur konsequenten Sicherheitspolitik**
- **Ernennung eines Sicherheitsbeauftragten auf Managementebene**
- **Einführung von Grundsätzen und Leitlinien**

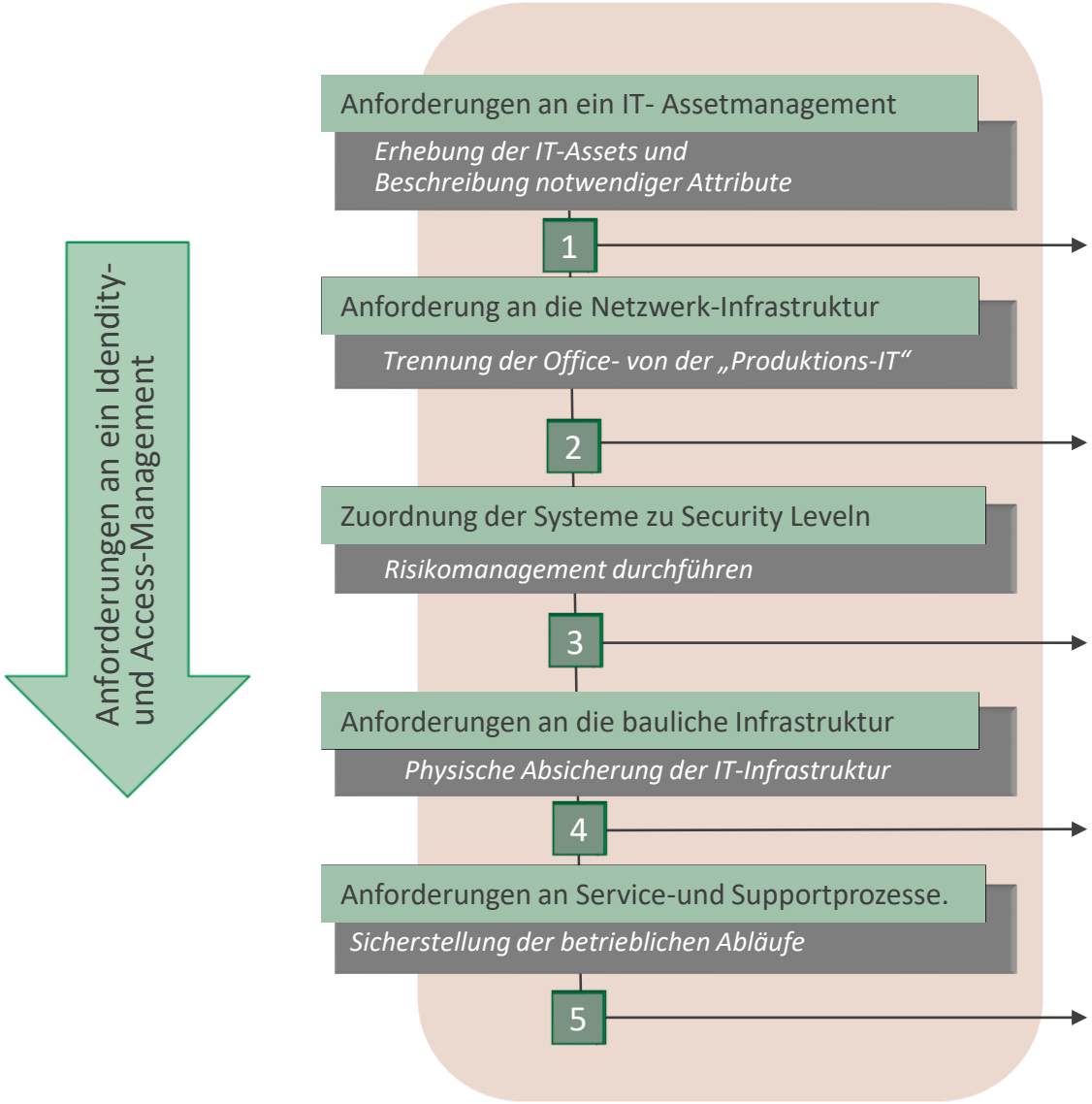
- **Implementierung der ISMS-Organisation**
- **Technik überprüfen und bewerten (Vulnerability Assessment)**
- **Ressourcen und Prozesse zugeordnen und bewerten**
- **Ggf. weitere branchenspezifische Assessments (z.B. ISO / TS 16949)**

- **Beurteilung der Prozesse nach „Business-Kritikalität“**
- **Erstellung eines Business-Blueprints der Systemlandschaft**
- **Ermittlung der Assetwerte zur Bildung eines Kennzahl-Systems**
- **Bedrohungs- und Schwachstellenanalyse der Systemlandschaft**
- **Bewertung der möglichen Risiken**
- **Erstellung eines Risikobegegnungsplans**

- **Entscheidung zur Akzeptanz oder Transfer von Risiken**
- **Durchführung von Sicherheitssofortmaßnahmen**
- **Anpassung des BCM zur Abdeckung operativer Risiken**

- **Terminierung und Initiierung notwendiger Projekte**
- **Überprüfung der Umsetzung eingeleiteter Maßnahmen**
- **Absicherung durch Etablierung des Notfallmanagements**

Vorgehen zur Regelung TECHNISCHER Absicherung



Beispiele für themenbezogene Schwerpunkte

(individuell abzustimmen)

- Anforderungen an Server und Endgeräte
- Anforderungen an aktive Komponenten
- Anforderungen. Aufnahme und Zuordnung von Applikationen zu IT-Assets
- Einbeziehung eines vorhandenen Assetmanagements und /oder einer CMDB

- Separierung der Office-Umgebung von den Produktions- (Netzleit-/Fernwirk-) Systemen
- Security Gateways (Firewalls, IDS/IDP)
- Anforderung an Sicherheitszonen
- Anforderungen an Fernzugriffe
- Anforderungen an Protokollierung und Überwachung

- Beurteilung der Systeme nach „Business-Kritikalität“ und Zuordnung zu Security-Leveln
- Definition der technischen Anforderungen an Security-Level
- Definition der organisatorischen Anforderungen an Security Level

- Anforderungen an Zugang- und Zutritt
- Anforderungen an bauliche Maßnahmen
- Anforderungen an organisatorische Maßnahmen (z.B. Brandschutz, EMA, etc.)

- Anforderungen an ein Security-Incident-Management
- Anforderungen an ein Change-Management
- Anforderungen an ein Configuration und Capacy Management
- Formaler Umgang mit Ausnahmen

Darstellung eines 2700x-Regelwerkes nach Best-Practice

Policy Datenschutz & Informationssicherheit

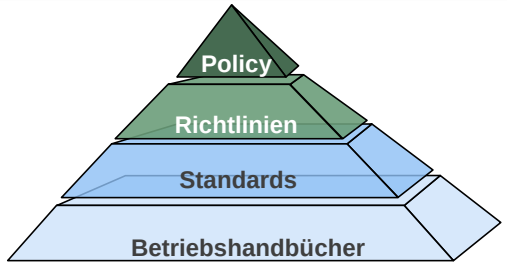
Richtlinie Datenschutz- & Informationssicherheitsmanagement

Richtlinie DS / IS Mitarbeiter

Standards

- IS Produktions-systeme
- IS Lokale Endgeräte
- IS Netzwerk-sicherheit (Kryptographie)
- IS Incident Management
- IS Risiko Management
- IS Klassifizierung
- IS Identity und Access Management
- IS Physische Sicherheit/ Lokale IT-Räume
- IS Business Continuity Management
- IS Personelle Sicherheit (Compliance, Datenschutz)
- IS Anwendungs-sicherheit (Change-Prozess)

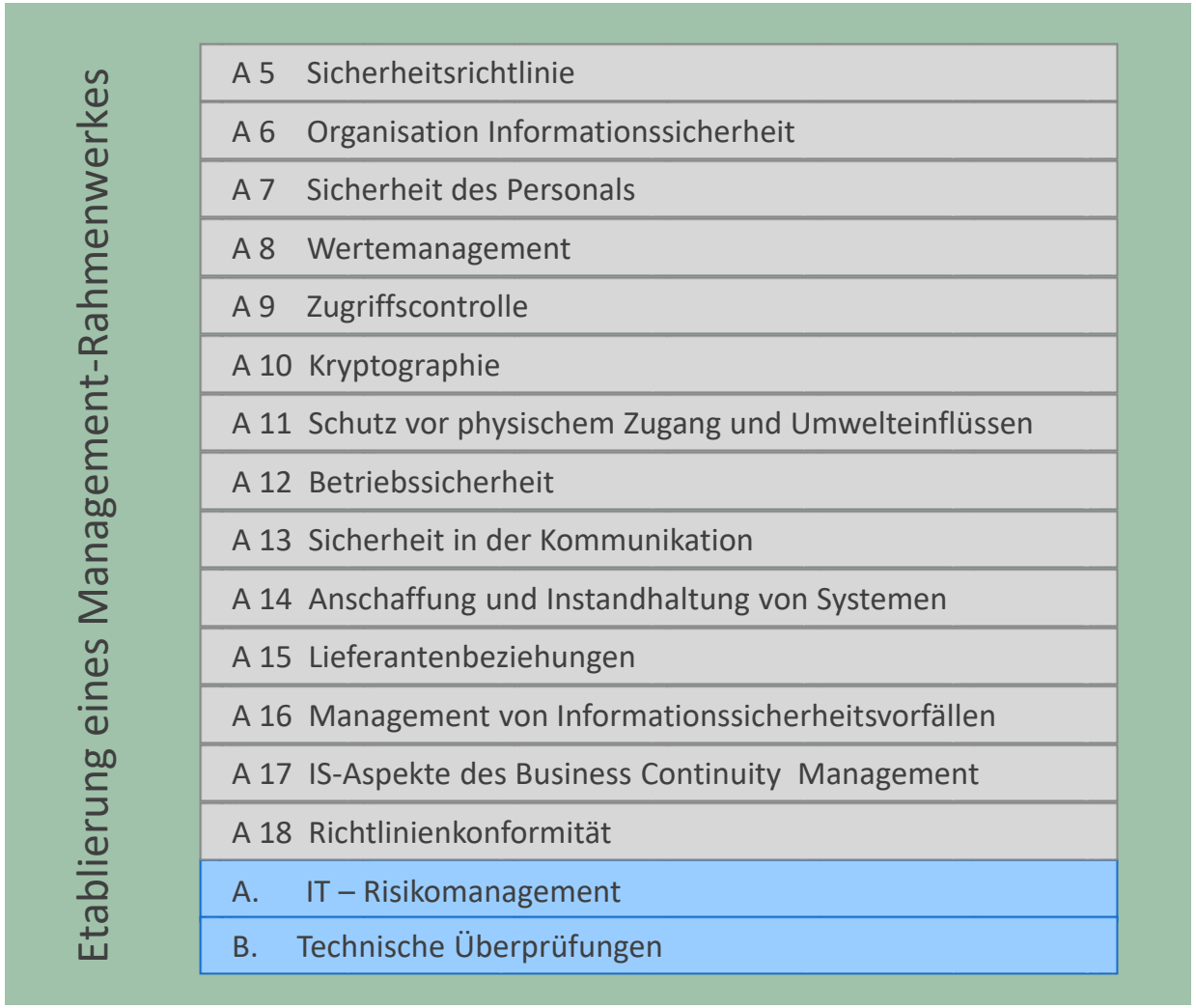
Dienstleistungserbringung durch Dritte/Lieferanten/Provider/Cloud-Dienstleister



IS = Informationssicherheit

ISO 27001 Controls

Abbildung der Normen in der QSEC Suite



- Komplette Darstellung der Norm z. B. ISO/IEC 27001:2013 D2015-03
- Fragenkatalog integriert (Auswahl nach ja/nein oder Spice 0-5)
- Beschreibungstexte ISO/IEC 27002:2013
- Maßnahmenvorschläge (BSI, Best Practice etc.)
- Mapping zu Risikoszenarien
- Musterdokumente
  - Template IS-Policy
  - Template Informationssicherheitsmanagement
  - Template IS-Risikomanagement
  - Template IS-Klassifizierung
  - Platzhalterdokumente für Zuordnung zur Norm ISO/IEC 27001:2013 (siehe Beispiel SoA-Bericht)

Informationssicherheit & Datenschutz

Informationen müssen klassifiziert werden!

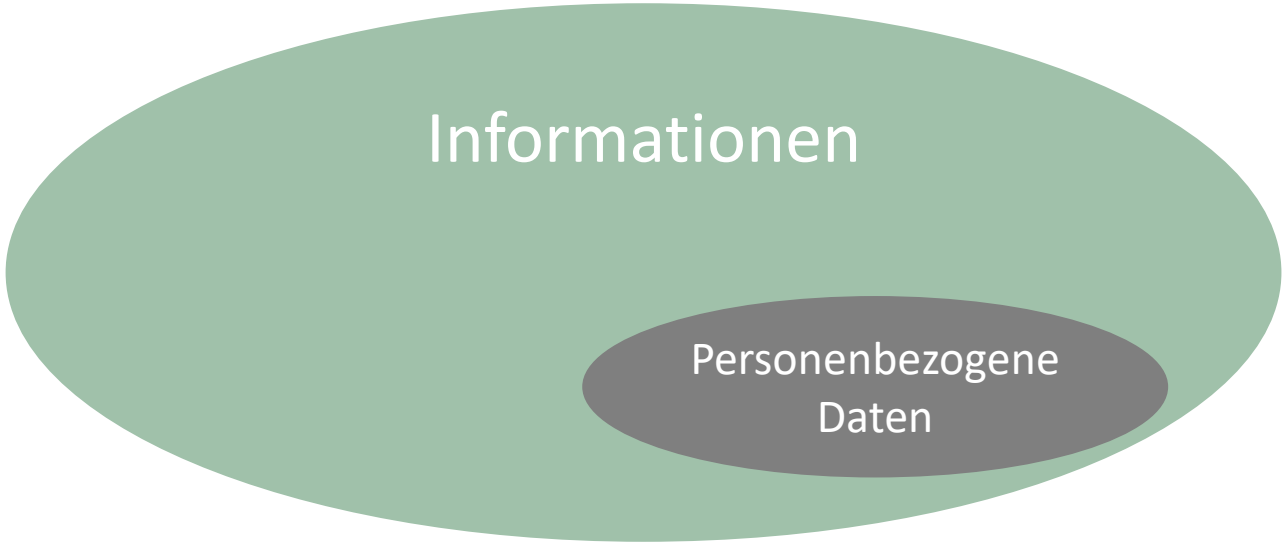
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Datenschutzrelevanz

verbunden

Geschäftsprozesse müssen bekannt sein

- Geschäftsprozesse
- Datenschutz verarbeitende Geschäftsprozesse
- Serviceprozesse

verarbeitet in



benötigt

Assets

Datenschutzbewertung mit QSEC

Bewertungsfelder für die „Rechenschaftspflicht“

Geschäftsprozesse

- Verantwortliche Stelle
- Zweckbestimmung
- Empfänger
- Belastbarkeit
- Privacy by Design
- Privacy by Default
- Folgenabschätzung
- Auftragsverarbeitung
- Zustimmungen
- Aufsichtsbehördenkontakt

Informationen

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Datenschutzrelevanz
  - Betroffene Personengruppen
  - Datenkategorien
  - Drittländer
  - Löschfristen
  - Zugriffsberechtigungen

Assets

- Assets die für die Datenschutz-Geschäftsprozesse benötigt werden
- Assets in denen die Informationen gespeichert werden

Maßnahmenkatalog (TOMs)
nach Stand der Technik

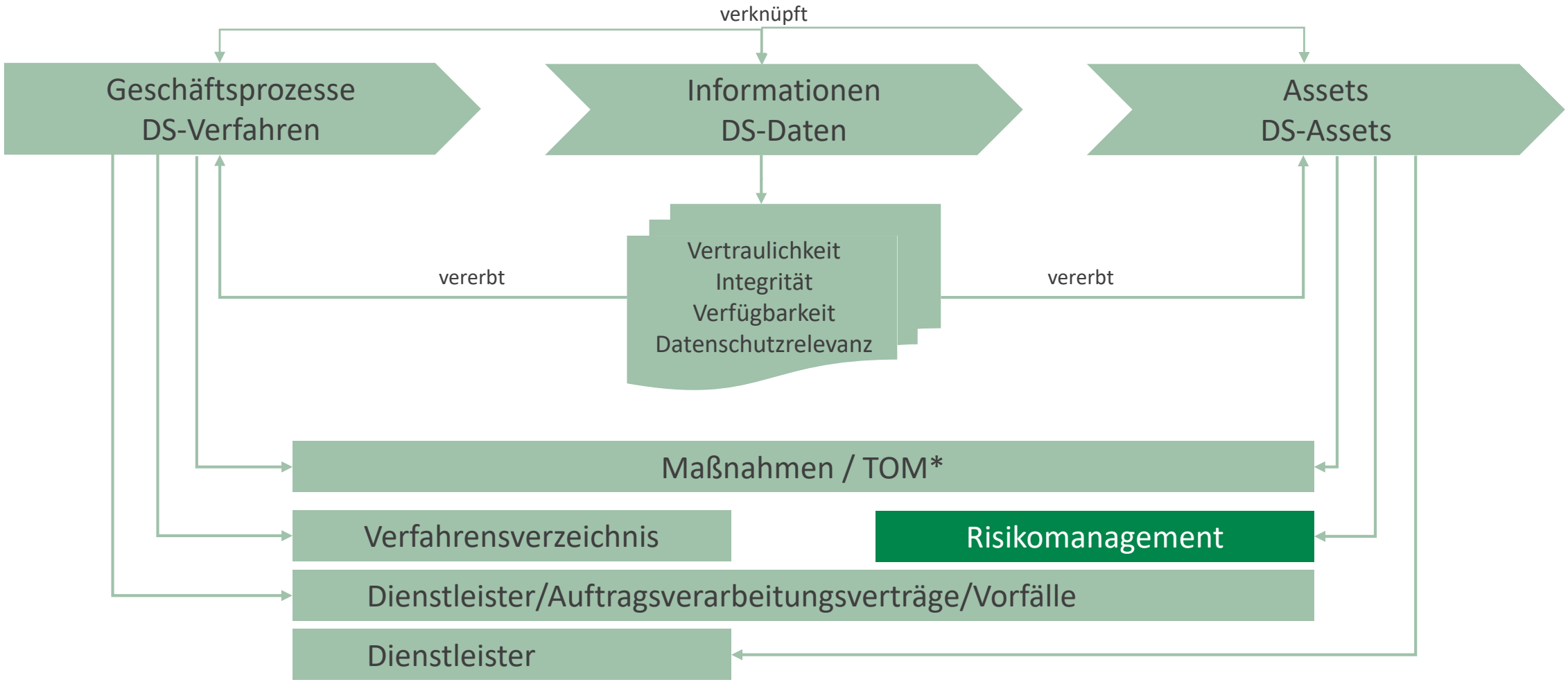
?

Technische und organisatorische Maßnahmen

Risikomanagement

QSEC - Methodisches Vorgehen

Alle Daten müssen verarbeitet werden



*TOM = Technisch Organisatorische Maßnahmen

ISO/IEC 27001:2013 D2015-03 Richtlinienzuordnung / Auszug

Anwendbarkeit der Norm 27001 auf den Scope / (SOA – Bericht)

ISO/IEC 27001:2013-D2015-03 Annex A		Erforderliche Aufgabe	Abwahlgrund	Auswahlgrund				Verknüpfte Dokumente
Control				LR	CO	BR/ BP	RRA	
A.5	Informationssicherheitsleitlinien							
A.5 .1	Vorgaben der Leitung zur Informationssicherheit							
A.5 .1.1	Informationssicherheitsrichtlinien	■		■	■	■		Policy Informationssicherheit_Platzhalter Richtlinie Informationssicherheit (-smanagement)_Platzhalter
A.5 .1.2	Überprüfung der Informationssicherheitsrichtlinien	■				■		Policy Informationssicherheit_Platzhalter Richtlinie Informationssicherheit (-smanagement)_Platzhalter Standard IS Klassifizierung_Platzhalter Standard IS Endgeräte_Platzhalter Standard IS Personelle Sicherheit (Compliance) (Datenschutz)_Platzhalter Standard IS Physische Sicherheit und lokale IT-Räume_Platzhalter Standard IS Identity und Access Management_Platzhalter Standard IS Anwendungssicherheit (Change-Prozess)_Platzhalter Standard IS Netzwerksicherheit und Kryptographie_Platzhalter Standard IS Dienstleistungserbringung durch Dritte_Platzhalter Standard IS Incident Management_Platzhalter Standard IS Business Continuity Management_Platzhalter
A.6	Organisation der Informationssicherheit							
A.6 .1	Interne Organisation							
A.6 .1.1	Informationssicherheitsrollen und -verantwortlichkeiten	■			■			Richtlinie Informationssicherheit (-smanagement)_Platzhalter
A.6 .1.2	Aufgabentrennung	■			■			Richtlinie Informationssicherheit (-smanagement)_Platzhalter
A.6 .1.3	Kontakt mit Behörden	■				■		Richtlinie Informationssicherheit (-smanagement)_Platzhalter
A.6 .1.4	Kontakt mit speziellen Interessensgruppen	■				■		Richtlinie Informationssicherheit (-smanagement)_Platzhalter
A.6 .1.5	Informationssicherheit im Projektmanagement	■				■		Richtlinie Informationssicherheit (-smanagement)_Platzhalter
A.6 .2	Mobilgeräte und Telearbeit							
A.6 .2.1	Richtlinie zu Mobilgeräten	■				■		Standard IS Endgeräte_Platzhalter
A.6 .2.2	Telearbeit	■		■				Standard IS Endgeräte_Platzhalter
A.7	Personalsicherheit							
A.7.1	Vor der Beschäftigung							
A.7.1.1	Sicherheitsüberprüfung	■				■		Standard IS Personelle Sicherheit (Compliance) (Datenschutz)_Platzhalter
A.7.1.2	Beschäftigungs- und Vertragsbedingungen	■				■		Standard IS Personelle Sicherheit (Compliance) (Datenschutz)_Platzhalter
A.7.2	Während der Beschäftigung							
A.7.2.1	Verantwortlichkeiten der Leitung	■				■		Standard IS Personelle Sicherheit (Compliance) (Datenschutz)_Platzhalter
A.7.2.2	Informationssicherheitsbewusstsein, -ausbildung und -schulung	■				■		Standard IS Personelle Sicherheit (Compliance) (Datenschutz)_Platzhalter
A.7.2.3	Maßregelungsprozess	■				■		Standard IS Personelle Sicherheit (Compliance) (Datenschutz)_Platzhalter
A.7.3	Beendigung und Änderung der Beschäftigung							
A.7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	■				■		Standard IS Personelle Sicherheit (Compliance) (Datenschutz)_Platzhalter

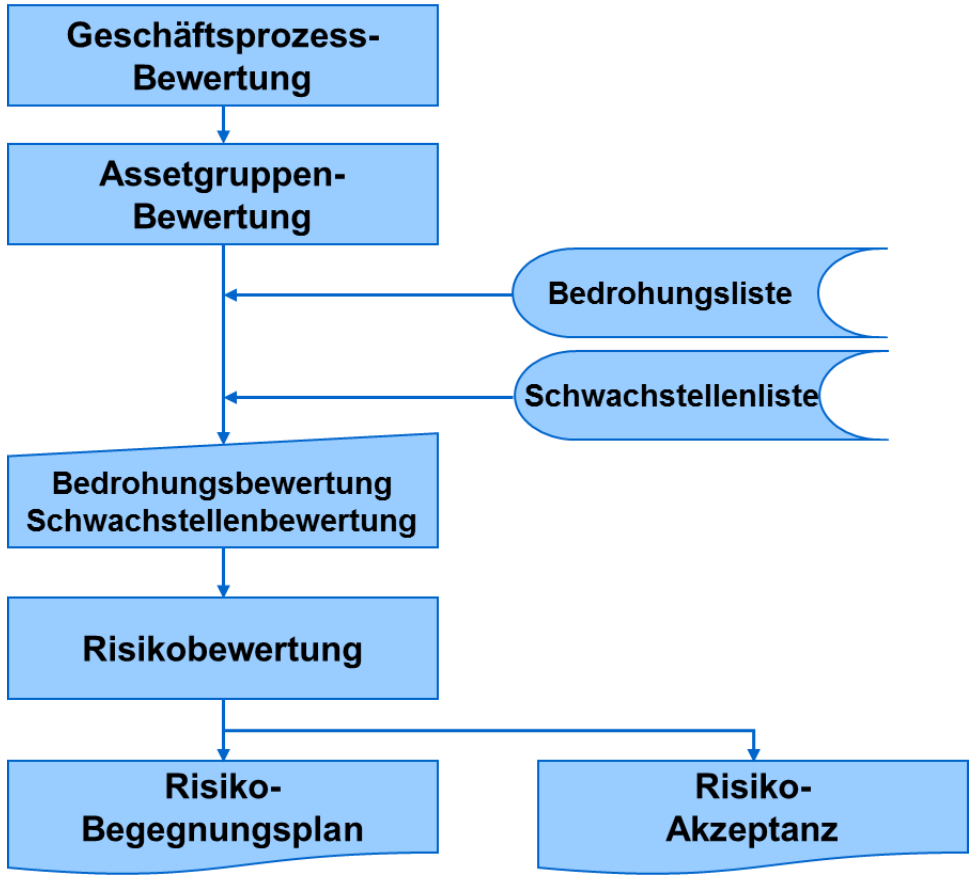
Risiko IT-bedingter Schäden
Risk Assessment Methode nach ISO/IEC 27005

Definition einer Vorgehensmethode

(Dokument Risk Assessment Methode)

Risk Assessment Aktivitäten (Ablaufplan)

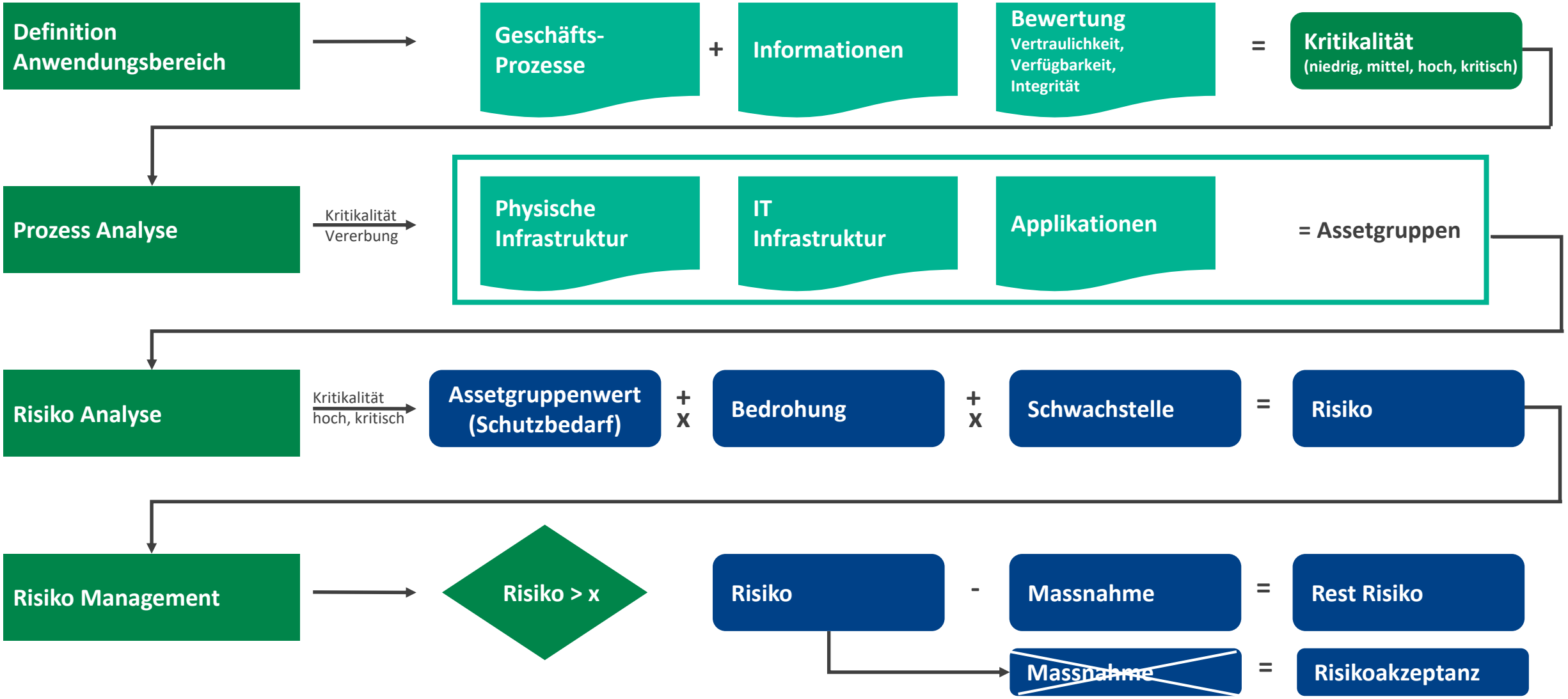
- Aufnahme der Systeme inkl. Klassifizierung resultierend aus den Geschäftsprozessen
- Identifikation der Bedrohungen
- Identifikation der Schwachstellen
- IST-Aufnahme der Gegenmaßnahmen
- Bestimmung der Eintrittswahrscheinlichkeiten
- Auswirkungsanalyse
- Risiko Beurteilung
- Empfehlung der Gegenmaßnahmen
- Ergebnisdokumentation



Risk Treatment Plan

Residual Risk Acceptance

Risiko Management



Beispiel Schutzbedarfsklassen Assetgruppen

Schutzbedarfsklassen 1-4 / niedrig, mittel, hoch, sehr hoch (kritisch)

Position	Bemessungsgröße	Möglicher Wertebereich	Beispiel Bewertung
A	Verfügbarkeit	1 = gering (> 24 Std.) 2 = normal (< 24 Std. > 8 Std.) 3 = erweitert (< 8 Std. > 2 Std.) 4 = permanent (< 2 Std.)	3
B	Integrität	1 = gering 2 = mittel 3 = hoch 4 = sehr hoch	4
C	Vertraulichkeit	1 = öffentlich 2 = intern 3 = vertraulich 4 = streng vertraulich/ persönlich	2
D	Geschätzter Schaden	1 = gering >0 T€ aber < 5.000 T€ 2= mittel > 5.000T€ aber < 10.000 T€ 3 = hoch >10.000 T€ aber < 15.000 T€ 4 = sehr hoch >15.000 T€ Errechnet aus max. V,I,V	4
E	Ergebnis: **Asset-Bewertung**	MAX (A,B,C)	4

Maximumprinzip aus V,I,V

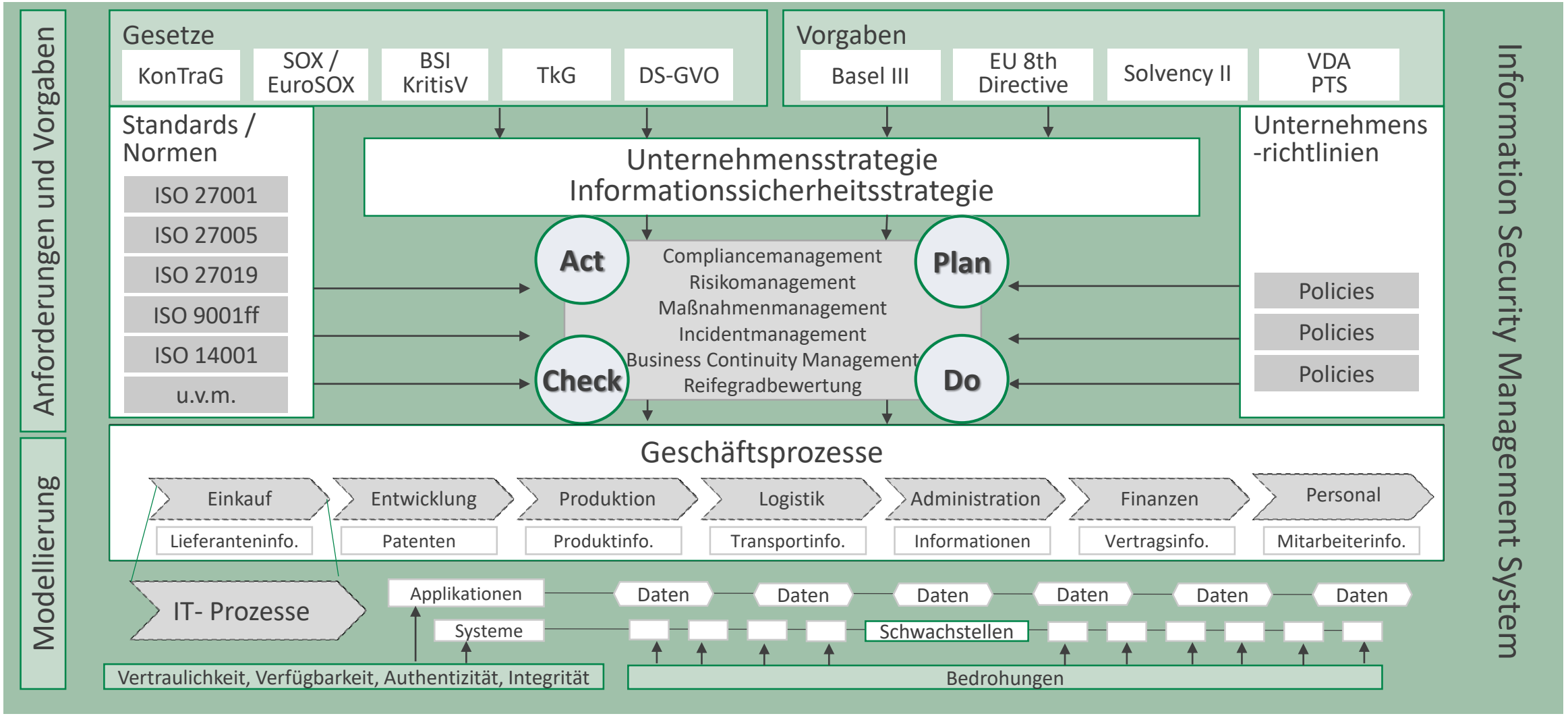
Risikostufenmatrix

Schadenswirkung (Schutzbedarf)		Schwachstelle		Risikostufe			
4	sehr hoch	4	leicht	C (16)	B (32)	B (48)	A (64)
3	hoch	3	mittel	C (9)	C (18)	B (27)	B (36)
2	mittel	2	gering	D (4)	C (8)	C (12)	C (24)
1	gering	1	schwer	D (1)	D (2)	C (3)	C (4)
				Sehr unwahrscheinlich	Weniger wahrscheinlich	Wahrscheinlich	Sehr wahrscheinlich
				1	2	3	4

Bedrohung

Risikowert	0	1	2	3	4	6	8	12	16	18	24	27	32	36	48	64
Risikostufe	D	D	D	D	D	C	C	C	C	C	C	B	B	B	B	A

Information Security Management System



Fazit

- Management-Commitment einholen
- Budget & Ressourcen festlegen
- Richten Sie jetzt ein Datenschutz-/ IS-Managementsystem ein
- Legen Sie die Methoden und Prozesse fest
- Führen Sie eine DS/ISMS-Software ein

Haben Sie Fragen? Kontaktieren Sie uns!

Besuchen Sie uns auf unserer Webseite und melden Sie sich zu einer QSEC-Live Präsentation oder rufen Sie uns an!

Ihr Ansprechpartner für Fragen:

Herr Werner Wüpper

Tel.: 040/650 336-11
Mobil: 0172 45 41 022
E-Mail: werner.wuepper@wmc-direkt.de

Wüpper Management Consulting GmbH im Internet:

http://wmc-direkt.de/grc-isms-software/online-demo